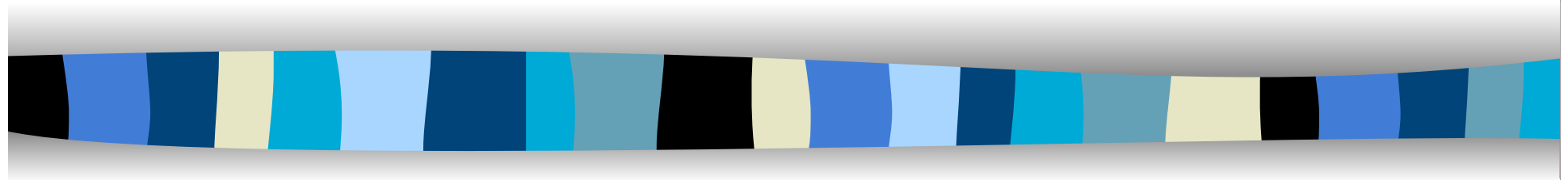


Formal Methods in software development



a.a.2017/2018

Prof. Anna Labella



Proving Equivalences

The bisimulation proof method:

To establish $P \approx Q$:

1. Identify a relation S such that $P S Q$
2. Prove that S is a weak bisimulation relation

This is the canonical method

There are other methods for process verification:

1. Modal logic specification/proof (see later)
2. Equational reasoning (rewriting method: see later)



Bisimilarity as a maximal fixed point

Let us take $Q \times Q$ to start with, then calculate

$F(Q \times Q) = \{ (q_1, q_2) \mid q_1 \rightarrow^\alpha q_1' \text{ implies } q_2 \rightarrow^\alpha q_2' \text{ and viceversa} \}$.

By iterating the procedure, we obtain a decreasing chain

$$\dots F^4(Q \times Q) \subseteq F^3(Q \times Q) \subseteq F^2(Q \times Q) \subseteq F(Q \times Q)$$

We can apply Tarski's theorem and obtain a maximal fixed point $S \subseteq Q \times Q$. The relation S is a strong bisimulation.

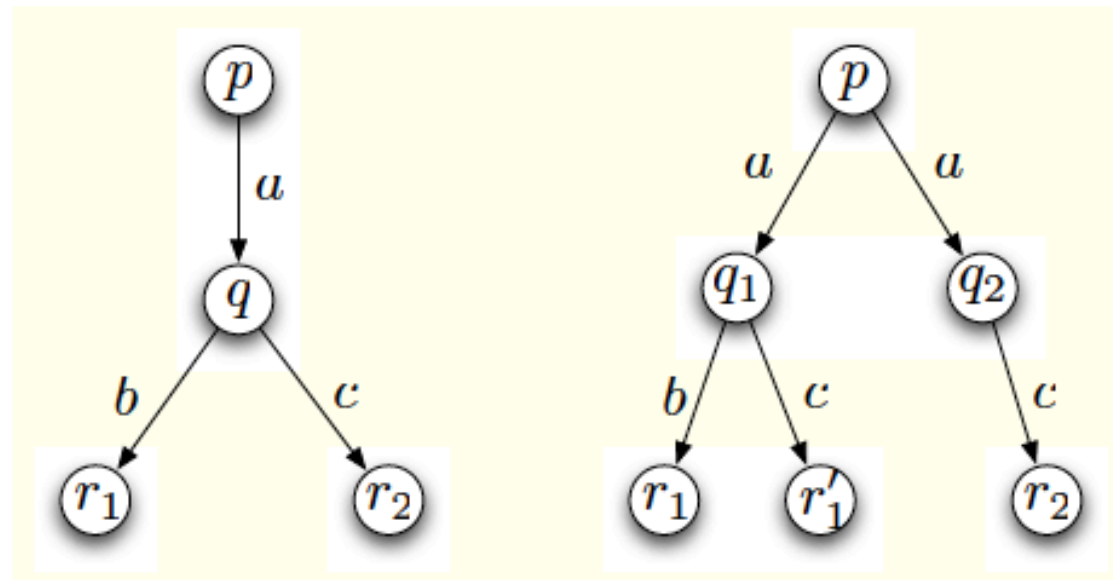
The same holds for weak bisimulation relation defining

$F(Q \times Q) = \{ (q_1, q_2) \mid q_1 \rightarrow^\alpha q_1' \text{ implies } q_2 \Rightarrow^\alpha q_2' \text{ and viceversa} \}$

Similarity and bisimilarity

Theorem 12. $\sim \subseteq \leq \cap \geq$ and in general the inclusion is strict.

Proof. Any bisimulation and its opposite are clearly simulations. On the other hand, the following example shows that bisimilarity is finer than simulation equivalence.





Bisimulation game, 1

We are given two LTSS $\mathcal{L}_1, \mathcal{L}_2$. The configuration is a pair of states (p, q) , $p \in \mathcal{L}_1, q \in \mathcal{L}_2$. The bisimulation game has two players: \mathcal{P} and \mathcal{R} . A round of the game proceeds as follows:

- (i) \mathcal{R} chooses either p or q ;
- (ii) assuming it chose p , it next chooses a transition $p \xrightarrow{a} p'$;
- (iii) \mathcal{P} must choose a transition with the same label in the other LTS, ie assuming \mathcal{R} chose p , it must find a transition $q \xrightarrow{a} q'$;
- (iv) the round is repeated, replacing (p, q) with (p', q') .



Bisimulation game, 2

Rules: An infinite game is a win for \mathcal{P} . \mathcal{R} wins iff the game gets into a round where \mathcal{P} cannot respond with a transition in step (iii).

Observation 10. *For each configuration (p, q) , either \mathcal{P} or \mathcal{R} has a winning strategy.*

Theorem 11. *$p \sim q$ iff \mathcal{P} has a winning strategy. ($p \approx q$ iff \mathcal{R} has a winning strategy.)*



\mathcal{P} has a winning strategy $\Rightarrow p \sim q$

Let $GE \stackrel{\text{def}}{=} \{ (p, q) \mid \mathcal{P} \text{ has a winning strategy} \}$.

Suppose that $(p, q) \in GE$ and $p \xrightarrow{a} p'$. Suppose that there does not exist a transition $q \xrightarrow{a} q'$ such that $(p', q') \in GE$. Then \mathcal{R} can choose the transition $p \xrightarrow{a} p'$ and \mathcal{P} cannot respond in a way which keeps him in a winnable position. But this contradicts the fact that \mathcal{P} has a winning strategy for the game starting with (p, q) . Thus GE is a bisimulation.

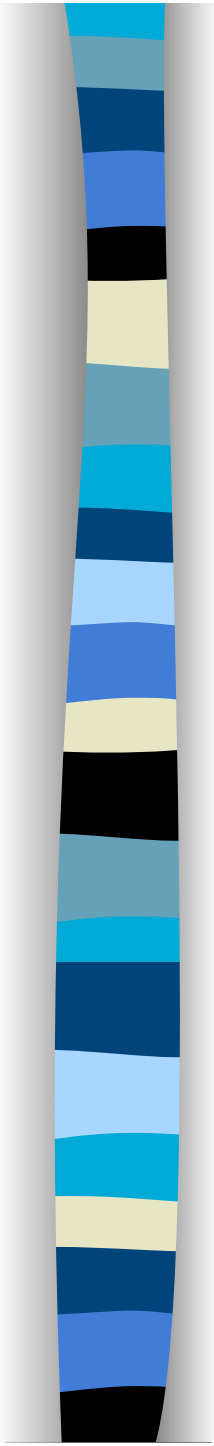


$p \sim q \Rightarrow \mathcal{P}$ has a winning strategy

Bisimulations are winning strategies:

If $p \sim q$ then there exists a bisimulation R such that $(p, q) \in R$.

Whatever move \mathcal{R} makes, \mathcal{P} can always make a move such that the result is in R . Clearly, this is a winning strategy for P .



**We will give a language, the so-called
Hennessy-Milner logic, which describes
observations/experiments on LTSs**

Hennessy Milner logic

Suppose that A is a set of actions. Let

$$L ::= [a]L \mid \langle a \rangle L \mid \neg L \mid L \vee L \mid L \wedge L \mid \top \mid \perp$$

Given an LTS we define the semantics by structural induction over the formula φ :

- $q \models [A]\varphi$ if for all q' such that $q \xrightarrow{a} q'$ we have $q' \models \varphi$;
- $q \models \langle A \rangle \varphi$ if there exists q' such that $q \xrightarrow{a} q'$ and $q' \models \varphi$;
- $q \models \neg \varphi$ if it is not the case that $q \models \varphi$;
- $q \models \varphi_1 \vee \varphi_2$ if $q \models \varphi_1$ or $q \models \varphi_2$;
- $q \models \varphi_1 \wedge \varphi_2$ if $q \models \varphi_1$ and $q \models \varphi_2$;
- $q \models \top$ always;
- • $q \models \perp$ never;



HM logic example formulas

- $\langle a \rangle \top$ – can perform a transition labelled with a ;
- $[a] \perp$ – cannot perform a transition labelled with a ;
- $\langle a \rangle [b] \perp$ – can perform a transition labelled with a to a state from which there are no b labelled transitions.
- $\langle a \rangle ([b] \perp \wedge \langle c \rangle \top)$ – ?

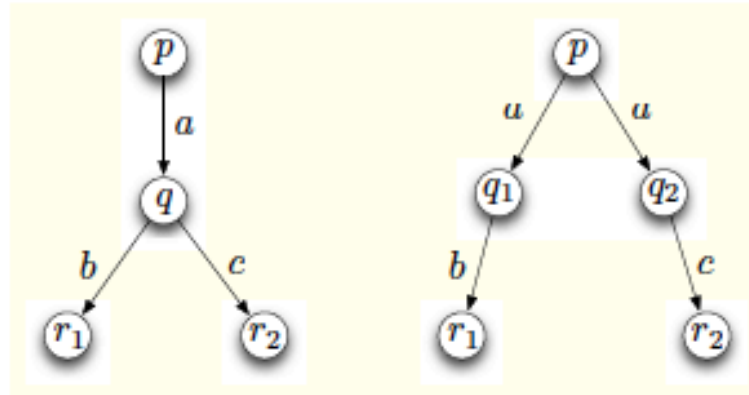
Basic properties of HM logic

Lemma 14 (“De Morgan” laws for HM logic).

- $[a] = \neg \langle a \rangle \neg$;
- $\langle a \rangle = \neg [a] \neg$;
- $\wedge = \neg(\neg \vee \neg)$;
- $\vee = \neg(\neg \wedge \neg)$;
- $\top = \neg \perp$;
- $\perp = \neg \top$.

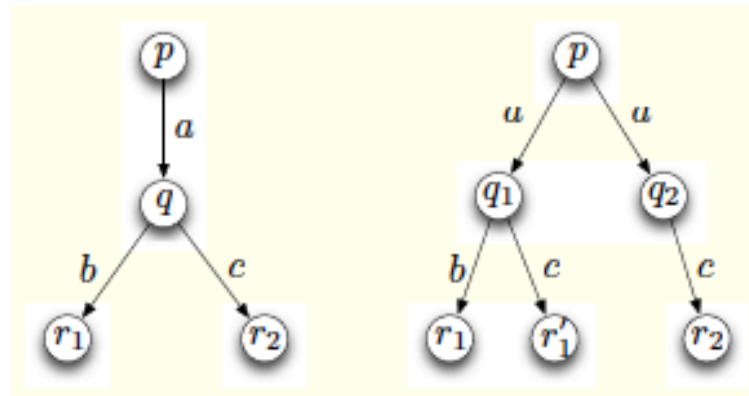
In particular, to get the full logic it suffices to consider just the subsets $\{\langle a \rangle, \vee, \perp, \neg\}$ or $\{[a], \wedge, \top, \neg\}$ or $\{\langle a \rangle, [a], \vee, \wedge, \top, \perp\}$.

Distinguishing formulas



$$\models \langle a \rangle (\langle b \rangle \wedge \langle c \rangle)$$

$$\not\models \langle a \rangle (\langle b \rangle \wedge \langle c \rangle)$$



$$\not\models \langle a \rangle (\neg \langle b \rangle)$$

$$\models \langle a \rangle (\neg \langle b \rangle)$$

Logical equivalence

Definition 15. *The logical preorder \leq_L is a relation on the states of an LTS defined as follows:*

$$p <_L q \text{ iff } \forall \varphi. p \models \varphi \Rightarrow q \models \varphi$$

It is clearly reflexive and transitive.

Definition 16. Logical equivalence is $\sim_L \stackrel{\text{def}}{=} \leq_L \cap \geq_L$. *It is an equivalence relation.*

Observation 17. *Actually, for HM, $\leq_L = \sim_L = \geq_L$. This is a consequence of having negation.*

Proof. Suppose $p \leq_L q$ and $q \models \varphi$. If $p \not\models \varphi$ then $p \models \neg\varphi$, hence $q \models \neg\varphi$ hence $q \not\models \varphi$, a contradiction. Hence $p \models \varphi$. □



Hennessy Milner & Bisimulation

Definition 18. An LTS is said to have **finite image** when from any state, the number of states reachable is finite.

Theorem 19 (Hennessy Milner). Let \mathcal{L} be an LTS with finite image. Then $\sim_L = \sim$.

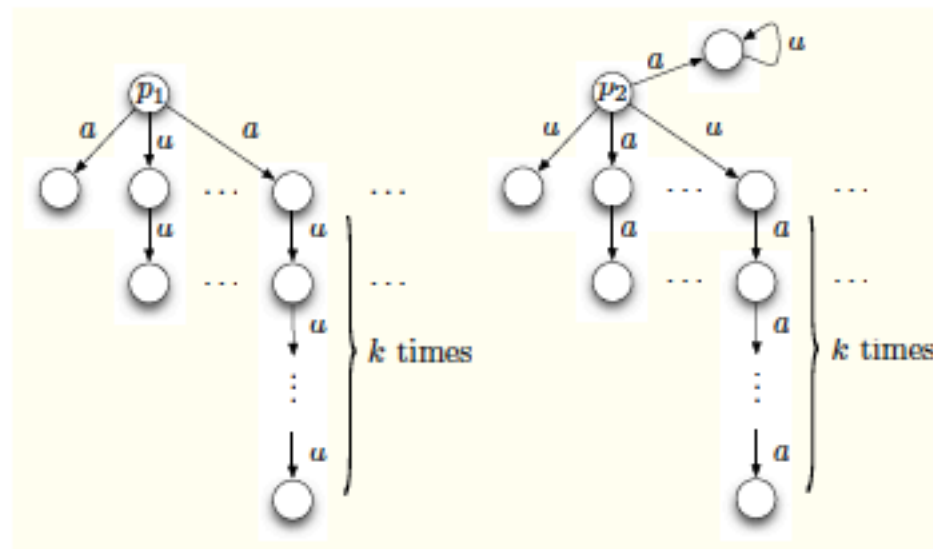
To prove this, we need to show:

- **Soundness** ($\sim_L \subseteq \sim$): If two states satisfy the same formulas then they are bisimilar.
- **Completeness** ($\sim \subseteq \sim_L$): If two states are bisimilar then they satisfy the same formulas.

Remark 20. Completeness holds in general. The finite image assumption is needed only for soundness.

Image finiteness

The theorem breaks down without this assumption:



Easy to check, using the bisimulation game, that $p_1 \approx p_2$.

Solution: Introduce infinite conjunction to the logic.

Soundness

$\sim_L \subseteq \sim$ (Soundness)

It suffices to show that \sim_L is a bisimulation. We will rely on image finiteness.

Suppose that $p \sim_L q$ and $p \xrightarrow{a} p'$. Then $p \models \langle a \rangle \top$ and so $q \models \langle a \rangle \top$ – thus there is at least one q' such that $q \xrightarrow{a} q'$. The set of all such q' is also finite by the extra assumption – let this set be $\{q_1, \dots, q_k\}$. Suppose that for all q_i we have that $p' \not\sim_L q_i$. Then $\exists \varphi_i$ such that $p' \models \varphi_i$ and $q_i \not\models \varphi_i$. Thus while $p \models \langle a \rangle \bigwedge_{i \leq k} \varphi_i$ we must have $q \not\models \langle a \rangle \bigwedge_{i \leq k} \varphi_i$, a contradiction. Hence there exists q_i such that $q \xrightarrow{a} q_i$ and $p' \sim_L q_i$.

Completeness 1

$\sim \subseteq \sim_L$ (Completeness)

We will show this $p <_L q$ by structural induction on formulas.

Base: $p \models \top$ then $q \models \top$. Also, $p \models \perp$ then $q \models \perp$.

Induction:

• Modalities ($\langle a \rangle$ and $[a]$):

- If $p \models \langle a \rangle \varphi$ then $p \xrightarrow{a} p'$ and $p' \models \varphi$. By assumption, there exists q' such that $q \xrightarrow{a} q'$ and $p' \sim q'$. By inductive hypothesis $q' \models \varphi$ and so $q \models \langle a \rangle \varphi$.
- If $p \models [a] \varphi$ then whenever $p \xrightarrow{a} p'$ then $p' \models \varphi$. First, notice that $p \sim q$ implies that if $q \xrightarrow{a} q'$ then there exists p' such that $p \xrightarrow{a} p'$ with $p' \sim q'$. Since $p' \models \varphi$, also $q' \models \varphi$. Hence $q \models [a] \varphi$.

Completeness 2

- Propositional connectives (\vee and \wedge):
 - if $p \models \varphi_1 \vee \varphi_2$ then $p \models \varphi_1$ or $p \models \varphi_2$. If it is the first then by the inductive hypothesis $q \models \varphi_1$, if the second then $q \models \varphi_2$; thus $q \models \varphi_1 \vee \varphi_2$.
 - if $p \models \varphi_1 \wedge \varphi_2$ is similar.

Note that completeness does not need the finite image assumption – thus bisimilar states *always* satisfy the same formulas. In the proof, we used the fact that $\{\langle a \rangle, [a], \vee, \wedge, \top, \perp\}$ is enough for all of HM logic.